JUNE 2025 | INSIGHT BRIEF

Advancing NATO's Digital Resilience

Strengthened public-private partnerships are key to securing critical infrastructure from cyber threats

Cloud providers, data centers, and platform ecosystems—often owned by private entities and hosted across borders—support critical functions in healthcare, energy, finance, and defense. As the SolarWinds breach showed, reliance on digital services expands the attack surface for malicious actors and magnifies the risks and consequences of cyberattacks on NATO's collective security. Publicly reported cyberattacks targeting critical infrastructure have risen globally by 668 percent following Russia's invasion of Ukraine. There were 727 recorded attacks on critical infrastructure in NATO member states between 2020 and 2024. Forty-four of these attacks targeted digital service providers; at least three of these attacks impacted critical infrastructure in more than one country. Against a backdrop of increasing threats, NATO's digital resilience has depended on a complex web of shared obligations among private actors, the Alliance, and member states whose cyber capabilities vary widely. In a dynamic threat environment, it is essential to define roles across NATO, member states, and the private sector in order to bolster digital resilience.

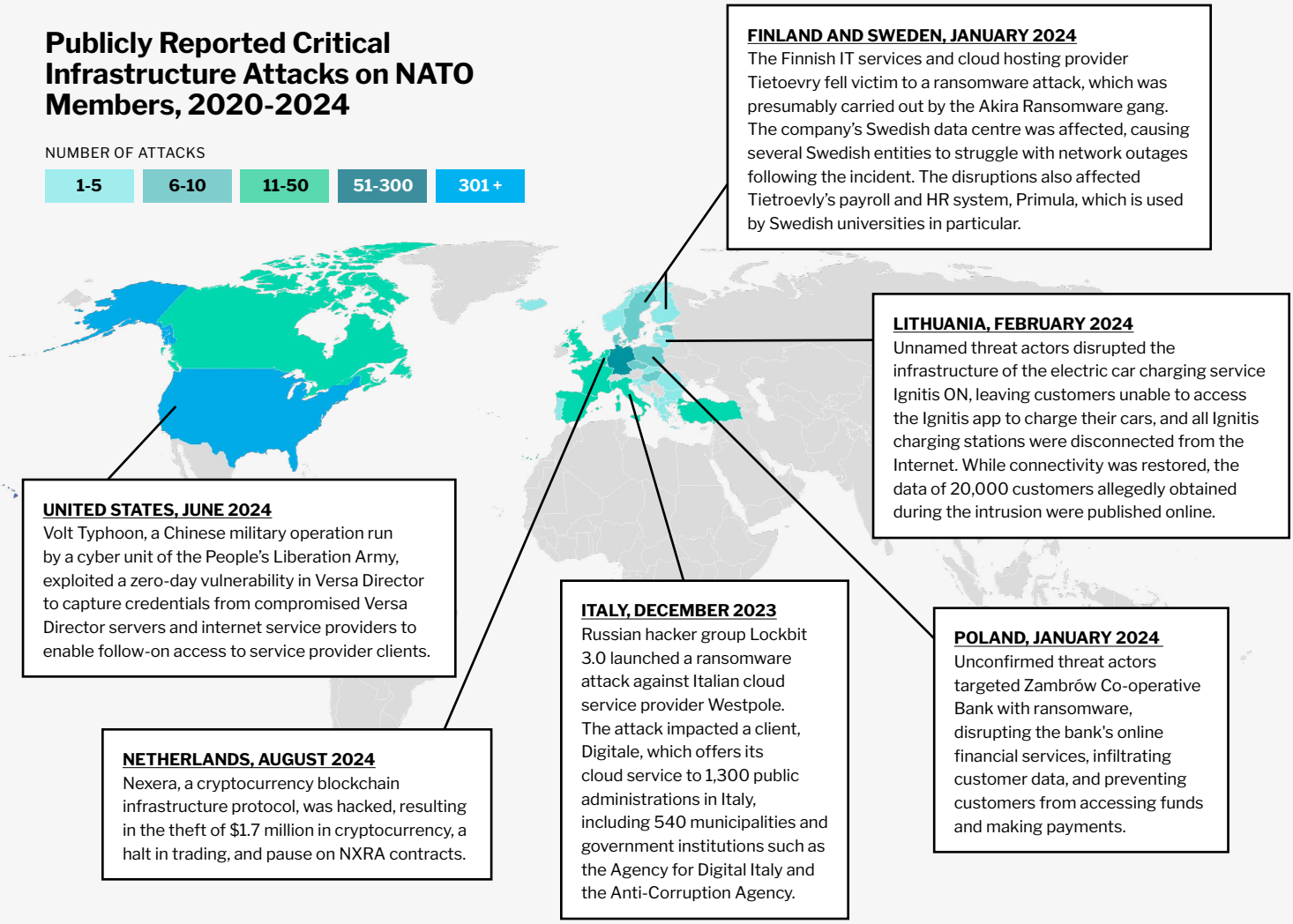
Cyber defense of digital infrastructure is a shared obligation among NATO, member governments, and the private sector.

NATO and its member states increasingly rely on privately operated digital systems and services that support logistics and command, facilitate surveillance, and store classified data. Beyond reliance, the private sector is rapidly becoming a strategic partner in ensuring European and NATO cyber defense and resilience. In Ukraine, Microsoft and Google's cloud services host threatened digital infrastructure to mitigate the impacts of Russian cyberattacks, representing a resilient, cloud-based defense model stemming from public-private cooperation.

Most allied governments contract national providers to build sovereign cloud services, resulting in a patchwork of systems that are often not interoperable. Guided by the Digital Transformation Implementation Strategy, NATO is pursuing new technical capabilities such as NATO Digital Backbone and its reference architecture, the Federated Mission Networking initiative, and the Allied software for cloud and Edge (ACE) to bridge these interoperability divides. However, the success of the initiatives hinges on private service providers ensuring "security by design" platforms that rely on cooperation between private developers and defense planners.

Yet, public-private cooperation is not guaranteed. The interests of commercial owners of critical infrastructure and digital services do not always align with the strategic priorities of governments or NATO. This potential disconnect represents a core vulnerability in the Alliance's digital defense posture. Although NATO has recognized that attacks against privately owned critical infrastructure could trigger Article 5, private owners of critical infrastructure are primarily responsible for the cybersecurity of their own institutions. Liability concerns, regulatory exposure, and unclear protocols may further hinder real-time threat sharing and coordination.

Publicly Reported Critical Infrastructure Attacks on NATO Members, 2020-2024



Governments and NATO have a responsibility to incentivize private sector cybersecurity hygiene and cooperation. The NATO Industry Cyber Partnership, the Cooperative Cyber Defence Centre of Excellence (CCDCOE), and the newly launched NATO Integrated Cyber Centre (NICC) signal growing institutional recognition of industry's crucial role. The NICC, announced at the 2024 Cyber Defence Conference, is expected to focus initially on shared situational awareness for Supreme Allied Commander Europe. Efforts to finalize its scope are ongoing, and ensuring tactical coordination and structured engagement with the private sector will be key to ensuring operational efficacy.

Looking Ahead

Building lasting digital resilience across NATO requires institutionalizing shared responsibilities, integrating private sector capabilities into security operations, and enforcing interoperability. This includes addressing uneven cyber capabilities and divergent policy approaches among member states, which complicate coordination and expose the alliance to systemic risks. To achieve this, the Alliance, its member states, and core partners can work to:

Institutionalize Threat Data Sharing: Build secure, cross-sector channels through the NICC to enable real-time intelligence exchange, and minimize legal and reputational risks for industry.
Formalize Public-Private Exercises: Integrate private digital providers into NATO planning, war-gaming, and stress-testing regimes.
Safeguard Technology for Peace and Humanitarian Outcomes: Support digital resilience of humanitarian operations in conflict settings through cross-sector collaboration among technology industry providers and the Alliance.

FP ANALYTICS | Microsoft

This insight brief was produced by FP Analytics, the independent research division of The FP Group, with support from Microsoft. FP Analytics retained control of the research direction and findings of the insight brief. Foreign Policy's editorial team was not involved in the creation of this content.